

IN THE CLAIMS:

Please cancel claims 1-36 without prejudice or disclaimer, and substitute new claims 37-72 therefor as follows:

Claims 1-36 (Cancelled).

37. (New) A method of preventing intrusion in communication traffic with a set of machines in a network, said traffic comprising communication entities, comprising the steps of:

providing a test system comprising test facilities replicating at least one of said machines in said set;

directing at least part of said communication entities in said traffic toward said test system;

running said communication entities directed toward said test system on said test facilities to detect possibly adverse effects on said test system, and

i) in the presence of an adverse effect, blocking the communication entities leading to said adverse effect, and

ii) in the absence of an adverse effect, allowing communication with said set of machines for the communication entities failing to lead to said adverse effect.

38. (New) The method of claim 37, wherein said at least part of said communication entities directed toward said test system include communication entities from traffic bound toward said set of machines.

39. (New) The method of claim 37, wherein said at least part of said communication entities directed toward said test system include communication entities from traffic coming from said set of machines.

40. (New) The method of claim 37, comprising the steps of:
providing a data base comprising patterns representative of forbidden communication entities for communication with said set of machines; and
blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base.

41. (New) The method of claim 37, comprising the steps of:
providing a further data base comprising patterns representative of allowed communication entities for communication with said set of machines; and
allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base.

42. (New) The method of claim 40, comprising the steps of:
detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base; and
directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base toward said test system to be run on said test facilities to detect possibly adverse effects on said test system.

43. (New) The method of claim 42, comprising, in the presence of said adverse effect, the step of adding to said data base the respective pattern identifying the communication entity leading to said adverse effect.

44. (New) The method of claim 41, comprising the steps of:

detecting unknown communication entities in said traffic as identified by
respective unknown patterns not included in said further data base; and

directing said unknown communication entities in said traffic as identified by
respective unknown patterns not included in said further data base toward said test
system to be run on said test facilities to detect possibly adverse effects on said test
system.

45. (New) The method of claim 44, comprising, in the absence of said adverse
effect, the step of adding to said further data base the respective pattern identifying the
communication entity failing to lead to said adverse effect.

46. (New) The method of claim 37, comprising, in the presence of said
adverse effect, the step of subjecting to a resetting step those of said test facilities in
said test system affected by said adverse effect.

47. (New) The method of claim 37, wherein the machines in said set comprise
facilities exposed to said adverse effect as well as additional contents, comprising the
step of configuring said test facilities in order to replicate said facilities exposed to said
adverse effect in the machines in said set.

48. (New) The method of claim 37, comprising the step of inhibiting said test
machines in said test system from providing responses to said traffic.

49. (New) The method of claim 37, comprising the steps of:
providing an in-line component ensuring said traffic with said set of machines;
and

providing at least one interface interfacing said in-line component with said test
system.

50. (New) The method of claim 49, comprising the step of providing feedback from said test system to said in-line component via said at least one interface.

51. (New) The method of claim 49, comprising the steps of:
providing a management network for managing said test system; and
providing feedback from said test system to said in-line component via said management network.

52. (New) The method of claim 43, comprising the steps of:
providing a parallel intrusion preventing arrangement including a respective data base including patterns representative of respective forbidden communication entities for communication with a respective set of machines; and
in the presence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect.

53. (New) The method of claim 45, comprising the steps of:
providing a parallel intrusion preventing arrangement including a respective further data base including patterns representative of respective allowed communication entities for communication with a respective set of machines; and
in the absence of said adverse effect, transmitting to said parallel intrusion preventing arrangement, for inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect.

54. (New) A system of preventing intrusion in communication traffic with a set of machines in a network, said traffic comprising communication entities, comprising:

a test system comprising test facilities replicating at least one of said machines in said set; and

a communication module configured for directing at least part of said communication entities in said traffic toward said test system, wherein said communication entities directed toward said test system are adapted to be run on said test facilities to detect possibly adverse effects on said test system,

said communication module being further configured for

i) in the presence of an adverse effect, blocking the communication entities leading to said adverse effect, and

ii) in the absence of an adverse effect, allowing communication with said set of machines for the communication entities failing to lead to said adverse effect.

55. (New) The system of claim 54, wherein said communication module is configured for including in said at least part of communication entities directed toward said test system communication entities from traffic bound toward said set of machines.

56. (New) The system of claim 54, wherein said communication module is configured for including in said at least part of communication entities directed toward said test system communication entities from traffic coming from said set of machines.

57. (New) The system of claim 54, comprising:
a data base comprising patterns representative of forbidden communication entities for communication with said set of machines; and
a firewall module configured for blocking forbidden communication entities in said traffic as identified by respective patterns included in said data base.

58. (New) The system of claim 54, comprising:

a further data base comprising patterns representative of allowed communication entities for communication with said set of machines,

said communication module being configured for allowing communication of allowed communication entities in said traffic as identified by respective patterns included in said further data base.

59. (New) The system of claim 57, wherein said communication module is configured for:

detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base; and

directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said data base toward said test system to be run on said test facilities to detect possibly adverse effects on said test system.

60. (New) The system of claim 59, wherein said communication module is configured for adding to said data base, in the presence of said adverse effect, the respective pattern identifying the communication entity leading to said adverse effect.

61. (New) The system of claim 58, wherein said communication module is configured for:

detecting unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base; and

directing said unknown communication entities in said traffic as identified by respective unknown patterns not included in said further data base toward said test system to be run on said test facilities to detect possibly adverse effects on said test system.

62. (New) The system of claim 61, wherein said communication module is configured for adding to said further data base, in the absence of said adverse effect, the respective pattern identifying the communication entity failing to lead to said adverse effect,

63. (New) The system of claim 54, wherein said test facilities in said test system are configured to undergo resetting following said adverse effect.

64. (New) The system of claim 54, wherein the machines in said set comprise facilities exposed to said adverse effect as well as additional contents, while said test facilities replicate said facilities exposed to said adverse effect in the machines in said set.

65. (New) The system of claim 54, wherein the test machines in said test system are inhibited from providing responses to said traffic.

66. (New) The system of claim 54, comprising:
an in-line component in said communication module ensuring said traffic with said set of machines, and
at least one interface interfacing said in-line component with said test system.

67. (New) The system of claim 66, wherein said test system is configured for providing feedback to said in-line component via said at least one interface.

68. (New) The system of claim 66, comprising a management network for managing said test system and said test system is configured for providing feedback to said in-line component via said management network.

69. (New) The system of claim 60, comprising an associated parallel intrusion preventing arrangement comprising a respective data base including patterns

representative of respective forbidden communication entities for communication with a respective set of machines, said communication module being configured for transmitting, in the presence of said adverse effect, to said parallel intrusion preventing arrangement, for inclusion in said respective data base, the respective pattern identifying the communication entity leading to said adverse effect.

70. (New) The system of claim 61, comprising an associated parallel intrusion preventing arrangement comprising a respective further data base comprising patterns representative of respective allowed communication entities for communication with a respective set of machines, said communication module is being configured for transmitting, in the absence of said adverse effect, said parallel intrusion preventing arrangement, for inclusion in said respective further data base, the respective pattern identifying the communication entity failing to lead to said adverse effect.

71. (New) A telecommunication network comprising the system of any one of claims 54 to 70.

72. (New) A computer program product loadable in the memory of at least one computer and including software portions capable of performing the steps of the method of any one of claims 37 to 53.